"Best Practices"
For
Improving Security

- Keep employees informed and promote a state of higher vigilance
- Require employees and visitors to wear IDs on company property
- Increase patrols and log security status by employees at company offices
- Monitor requests for system information from outside sources-Require that all information requests be in writing on company letterhead and only give out information with management approval
- Conduct communication checks on a periodic basis and provide additional communication devices; i.e., radios, cell phones, etc., for employees
- Encourage employees to be aware of their surroundings while working on system facilities
- Increase patrols and log security status of employees around the system
- Encourage employees to take all system alarms, routine or otherwise, seriously and investigate the alarms to verify system status
- Meet with local, state, federal, and possibly military law enforcement to increase awareness and to assist in patrolling key facilities and responding to emergencies
- Develop threat response levels to ensure response is appropriate to threat
- Develop security and staffing procedures relative to each of the threat levels
- Install new or additional protective barriers to manage and protect access to aboveground facilities as needed
- Add third-party security forces if needed
- Add additional electronic surveillance equipment such as cameras, motion alarms, etc., as needed
- Increase use of SCADA systems to monitor system operating conditions at critical facilities
- Change locks on all facilities to better manage access—review possible use of programmable and other high security locking devices
- Lock all valves (critical or non-critical) at aboveground facilities
- Secure all company equipment (valve keys, etc.) vehicle supplies, and vehicles when not in use
- Inventory company critical tools and equipment and manage more closely to prevent theft and use by unauthorized persons
- Limit access to excavations around facilities and do not leave the excavation open for extended periods of time
- Monitor excavation activities around critical facilities
- Conduct table top exercises, field exercises, mock disaster drills
- Have adequate tools, and equipment in inventory to repair or replace critical and/or site specific emergency response equipment
- Establish alternate communication systems in event of primary communication system failure

- Review alternate access routes to critical infrastructure in case primary route is unavailable
- Stage equipment to allow quick response—example, what if tunnels or bridges are not accessible?
- Determine what “out of the ordinary” equipment may be necessary to ensure access
- Meet with contractors in your area to evaluate what equipment they may have for use in the event of emergency
- Provide for alternate power supplies and periodically test them to ensure operation
- Have adequate vehicle and equipment logistics available-fuel, tires, spares, etc.
- Frequently meet with local law enforcement officials and health officials to discuss preparedness plans

This list of best practices is offered solely for informational purposes and should not be considered a complete or exhaustive list of practices for any individual utility operation. Evaluation and management of various types of risks is the responsibility of each utility.